

1
2
3
4
5
6 **IN THE UNITED STATES DISTRICT COURT**
7 **FOR THE WESTERN DISTRICT OF WASHINGTON**
8 **AT SEATTLE**

9 LEO GUY, individually and on behalf all
10 others similarly situated,

11 Plaintiffs,

12 v.

13 CONVERGENT OUTSOURCING, INC.,

14 Defendant.

No.

CLASS ACTION COMPLAINT

JURY DEMAND

15 **CLASS ACTION COMPLAINT**

16 Plaintiff(s) Leo Guy (“Plaintiff(s)”) bring this action, on behalf of themselves and all
17 others similarly situated, against Defendant Convergent Outsourcing, Inc. (“Convergent” or
18 “Defendant”). Plaintiff(s) seek to obtain damages, restitution, and injunctive relief for a class of
19 individuals (“Class” or “Class Members”) who are similarly situated and have received notices
20 of the data breach from Convergent. Plaintiff(s) make the following allegations upon information
21 and belief, except as to their own actions, the investigation of their counsel, and the facts that are
22 a matter of public record.

23 **I. NATURE OF THE ACTION**

24 1. This class action arises out of a 2022 data breach (“Data Breach”) of documents
and information stored on the computer network of Convergent, a third-party debt collection
company that serves the telecommunication, utility, banking, cable company, and financial

1 service industries by offering consumer debt collection.¹

2 2. According to its website, “Convergent believe[s] in customer service”² and claims
3 “[they] want to make it easy as possible for people to pay the debts they owe.”³

4 3. On its computer network, Convergent holds and stores certain highly sensitive
5 personally identifiable information (“PII” or “Private Information”) of the Plaintiff(s) and the
6 putative Class Members, who are customers of companies that Convergent provides debt
7 collection services for, i.e., individuals who provided their highly sensitive and private
8 information in exchange for business services.

9 4. According to the Notice of Data Breach Letter that Convergent sent to Plaintiff(s)
10 and Class members, it first became aware of the Data Breach on June 17, 2022, and began
11 investigating.⁴

12 5. Convergent finally began notifying the unknown or undisclosed number of
13 victims over 4 months after the “data breach” occurred, stating that their PII had been stolen in
14 what Defendant calls an “interruption to certain services performed by Convergent affecting
15 certain computer systems.”⁵

16 6. Convergent also admits that “an external actor gained unauthorized access to our
17 systems and deployed a ransomware malware” and that its “investigation also revealed that the
18 unauthorized actor deployed certain data extraction tools on one storage drive that is used to save
19 and share files internally.”⁶

20 7. As a result of Convergent’s Data Breach, Plaintiff(s) and thousands (if not more)
21 of Class Members suffered ascertainable losses in the form of the loss of the benefit of their
22 bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or
23

24 ¹ <https://www.convergentusa.com/outsourcing/question/list?type=A> (last accessed November 1, 2022)

² <https://www.convergentusa.com/outsourcing/site/who-is-convergent-outsourcing> (last accessed on November 1, 2022).

³ *Id.*

⁴ See Exhibit A, Plaintiff(s)’ Notice Letter.

⁵ *Id.*

⁶ *Id.*

1 mitigate the effects of the attack.

2 8. In addition, Plaintiff(s)' and Class Members' sensitive personal information—
3 which was entrusted to Defendant—who claims in the Data Breach Letter that “[they] take the
4 confidentiality, privacy, and security of information in our care seriously”⁷—was compromised
5 and unlawfully accessed and extracted during the Data Breach.

6 9. Based upon Convergent's notice letter, the Private Information compromised in
7 the Data Breach was intentionally accessed and removed, also called exfiltrated, by the cyber-
8 criminals who perpetrated this attack and remains in the hands of those cyber-criminals.

9 10. The Data Breach was a direct result of Defendant's failure to implement adequate
10 and reasonable cyber-security procedures and protocols necessary to protect Plaintiff(s) and
11 Class Members' Private Information.

12 11. Plaintiff(s) bring this class action lawsuit on behalf of those similarly situated to
13 address Defendant's inadequate safeguarding of Class Members' Private Information that they
14 collected and maintained, and for failing to provide timely and adequate notice to Plaintiff(s) and
15 other Class Members that their information had been subject to the unauthorized access of an
16 unknown third party and precisely what specific type of information was accessed.

17 12. Defendant maintained the Private Information in a reckless manner. In particular,
18 the Private Information was maintained on Defendant's computer network in a condition
19 vulnerable to cyberattacks. The mechanism of the cyberattack and potential for improper
20 disclosure of Plaintiff(s)' and Class Members' Private Information was a known risk to
21 Defendant. Thus, Defendant was on notice that failing to take steps necessary to secure the
22 Private Information from those risks left that property in a dangerous condition.

23 13. Defendant disregarded the privacy and property rights of Plaintiff(s) and Class
24 Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate
25 and reasonable measures to ensure its data systems were protected against unauthorized

⁷ *Id.*

1 intrusions; failing to disclose that they did not have adequately robust computer systems and
2 security practices to safeguard Class Members' Private Information; failing to take standard and
3 reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff(s) and
4 Class Members prompt and accurate and complete notice of the Data Breach.

5 14. In addition, Defendant and its employees failed to properly monitor the computer
6 network and systems that housed the Private Information. Had Defendant properly monitored its
7 computers, it would have discovered the intrusion sooner, and potentially been able to mitigate
8 the injuries to Plaintiff(s) and the Class.

9 15. Plaintiff(s)' and Class Members' identities are now at substantial and imminent
10 risk because of Defendant's negligent conduct since the Private Information that Defendant
11 collected and maintained (including Social Security numbers) is now in the hands of data thieves.

12 16. Armed with the Private Information accessed in the Data Breach, data thieves can
13 commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members'
14 names, taking out loans in Class Members' names, using Class Members' information to obtain
15 government benefits, filing fraudulent tax returns using Class Members' information, filing false
16 medical claims using Class Members' information, obtaining driver's licenses in Class Members'
17 names but with another person's photograph, and giving false information to police during an
18 arrest.

19 17. As a result of the Data Breach, Plaintiff(s) and Class Members have been exposed
20 to a heightened and imminent risk of fraud and identity theft. Plaintiff(s) and Class Members
21 must now and in the future closely monitor their financial accounts to guard against identity theft.

22 18. Plaintiff(s) and Class Members may also incur out of pocket costs for, *e.g.*,
23 purchasing credit monitoring services, credit freezes, credit reports, or other protective measures
24 to deter and detect identity theft.

19. Through this Complaint, Plaintiff(s) seek to remedy these harms on behalf of
themselves and all similarly situated individuals whose Private Information was accessed during
the Data Breach (the "Class").

20. Accordingly, Plaintiff(s) bring this action against Defendant for negligence, negligence per se, breach of implied contract, unjust enrichment, and declaratory relief, seeking redress for Convergent's unlawful conduct.

21. Plaintiff(s) seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate, long term credit monitoring services funded by Defendant, and declaratory relief.

II. PARTIES

22. Plaintiff Leo Guy is, and at all times relevant to this Complaint was, an individual citizen of the State of New Hampshire, residing in the city of Derry (Rockingham County). On or about October 31, 2022, Plaintiff Guy received a Notice of the Data Breach from Convergent Outsourcing, Inc. A copy of the notice they received is dated October 26, 2022, and attached as Exhibit A (the "Notice Letter").

23. Defendant Convergent Outsourcing, Inc., is a Washington for-profit corporation. Convergent's principal place of business is located at 800 SW 39th Street, Suite 100, Renton, Washington 98057. Defendant can be served through its registered agent at: CT Corporation System, 711 Capitol Way South, Suite 204, Olympia, Washington 98501.

24. According to its notice letter, the business operations of Convergent's affiliate, Account Control Technology, Inc. ("ACT") were also affected by the same Data Breach.⁸ Upon information and belief, both Convergent and ACT are subsidiaries of Account Control Technology Holdings, Inc.⁹

25. All of Plaintiff(s)' claims stated herein are asserted against Defendant Convergent, and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

26. This Court has subject matter jurisdiction over this action under 28 U.S.C.

⁸ *Id.*

⁹ <https://accountcontrol.com/About-Us/History> (last accessed November 1, 2022).

§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

27. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business or business venture in Washington; it is registered with the Secretary of State in Washington as a for-profit corporation; it maintains its headquarters in Washington; and committed tortious acts in Washington.

28. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district within which Convergent has the most significant contacts.

IV. STATEMENT OF FACTS

Nature of Defendant's Business.

29. Convergent started its business as a debt collection agency in 1950. Convergent has approximately 1,000 employees globally in the United States, Asia, Europe, and Africa while maintaining its headquarters in Renton, Washington.¹⁰

30. Prior to collecting consumer debt, Convergent collects PII of consumers from companies seeking Convergent's debt collection services. This PII includes, *inter alia*, consumers' names, contact information, Social Security numbers, and financial account information.

31. Convergent, in the regular course of its business, collects and maintains the PII of consumers (on behalf of its customers) as a requirement of its business practices.

32. Consumers entrusted the customers of Convergent with their PII with the mutual understanding that this highly sensitive private information was confidential and would be properly safeguarded from misuse and theft.

¹⁰ <https://www.zoominfo.com/pic/convergent-outsourcing/9502974> (last accessed November 1, 2022).

1 33. Convergent promises in its Privacy Policy that they “incorporate commercially
2 reasonable safeguards to help protect and secure your Personal Information.”¹¹

3 34. In its California Online Privacy Policy, Convergent acknowledges that it is
4 susceptible to data breaches and ransomware threats, acknowledging it must “detect security
5 incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting
6 those responsible for that activity.”¹² Moreover, Convergent is aware that it must: comply with
7 federal, state, and local laws; protect the safety, rights, property or security of consumers and
8 third parties; and detect, prevent, or otherwise address fraud, security, or technical issues.¹³

9 35. In the course of collecting Private Information from consumers, including
10 Plaintiff(s) and Class Members, Convergent promised to provide confidentiality and adequate
11 security for Private Information through its applicable Privacy Policy and in compliance with
12 statutory privacy requirements applicable to the servicing industry.

13 36. In its Notice Letters to Plaintiff(s) and Class Members, Convergent claims that
14 “the confidentiality, privacy, and security of information in our care are among our highest
15 priorities.”¹⁴

16 37. Plaintiff(s) and the Class Members, as consumers, relied on the promises and
17 duties of Convergent to keep their sensitive PII confidential and securely maintained, to use this
18 information for business purposes only, and to make only authorized disclosures of this
19 information. Consumers, in general, demand that businesses that require highly sensitive PII will
20 provide security to safeguard their PII, especially when Social Security numbers are involved.

21 38. In the course of their dealings, Plaintiff(s) and Class Members provided
22 Convergent (either directly or through Convergent’s business customers) with all or most of the
23 following types of Private Information:
24

¹¹ <https://www.convergentusa.com/outsourcing/page/privacy-policy> (last accessed on November 1, 2022).

¹² <https://www.convergentusa.com/outsourcing/page/ccpa-policy> (last accessed on November 1, 2022).

¹³ *Id.*

¹⁴ See Notice Letter, Ex. A.

- First and last names;
- Home addresses;
- Email addresses;
- Phone numbers;
- Social Security numbers;
- Employers;
- Account numbers; and
- Bank account or payment card information.¹⁵

39. Convergent had a duty to adopt reasonable measures to protect Plaintiff(s)' and Class Members' PII from unauthorized disclosure to third parties.

The Data Breach.

40. According to its Notice Letters, on June 17, 2022, Convergent "became aware of an interruption to certain services." After an unspecified amount of time, between the date they "became aware" and sent the notice letters, its investigation determined that an "unauthorized actor" accessed the Convergent network and "deployed certain extraction tools on one storage drive that is used to save and share files internally."¹⁶

41. The letter does not identify how long before detection the "interruption" was occurring.¹⁷

42. By October 26, 2022, according to Convergent's own Notice Letters, it was aware that the Data Breach included "name[s], contact information, financial account number[s], Social Security number[s],"¹⁸ including that of Plaintiff(s). Convergent does not why the Notice Letters were not sent until over 4 months later, time which could have helped Plaintiff(s) and Class members mitigate the damages suffered from Convergent's Data Breach.

¹⁵ See *id.*; see also <https://www.convergentusa.com/outsourcing/page/privacy-policy> (last accessed on November 1, 2022).

¹⁶ Notice Letter, Ex. A.

¹⁷ *Id.*

¹⁸ *Id.*

43. A review of various State Attorneys General websites shows that, to-date, Convergent has not yet notified the State Attorney Generals of this Data Breach, as required by the laws of the states.¹⁹ Convergent did not notify government agencies or the public about the Data Breach except through the Notice letters received by Plaintiff(s) and Class members over 4 months after the breach was discovered.

44. Moreover, Convergent has failed to expeditiously report how many individuals' records were exfiltrated during its Data Breach, as required by various state's laws.²⁰

45. Therefore, *Plaintiff(s)'s and Class members' PII was in the hands of cybercriminals for over 4 months before they were notified* of Convergent's Data Breach. Time is of the essence when trying to protect against identity theft after a data breach, so early notification is critical.

46. Because of this targeted, intentional cyberattack, data thieves were able to gain access to and obtain data from Convergent that included the Private Information of Plaintiff(s) and Class Members.

47. Convergent admits that the files exfiltrated from Convergent contained at least the following information of Plaintiff(s) and Class Members: names, contact information, financial account numbers, and Social Security numbers.

48. Upon information and belief, the Private Information stored on Convergent's network was not encrypted.

49. Plaintiff(s)' Private Information was accessed and stolen in the Data Breach. Plaintiff(s) reasonably believe their stolen Private Information is currently available for sale on

¹⁹ See, e.g., Maine: <https://apps.web.maine.gov/online/aeviewer/ME/40/list.shtml> showing "No entries found"; Texas: <https://oagtx.force.com/datasecuritybreachreport/apex/DataSecurityReportsPage> showing "No matching records found"; California: https://oag.ca.gov/privacy/databreach/list?field_sb24_org_name_value=convergent&field_sb24_breach_date_value%5Bmin%5D%5Bdate%5D=&field_sb24_breach_date_value%5Bmax%5D%5Bdate%5D= "There are currently no published reported breaches" (last accessed on November 1, 2022).

²⁰ See, e.g., Maine's requirements at https://www.maine.gov/ag/consumer/identity_theft/index.shtml (last accessed on November 1, 2022).

1 the Dark Web because that is the *modus operandi* of cybercriminals who target businesses that
2 collect highly sensitive Private Information.

3 50. As a result of the Data Breach, Convergent now encourages Class Members to
4 enroll in credit monitoring, fraud consultation, and identity theft restoration services, a tacit
5 admission of the imminent risk of identity theft faced by Plaintiff(s) and Class members.²¹

6 51. That Convergent is encouraging Plaintiff(s) and Class Members to enroll in credit
7 monitoring and identity theft restoration services is an acknowledgment that the impacted
8 consumers are subject to a substantial and imminent threat of fraud and identity theft.

9 52. Convergent had obligations created by contract, industry standards, and common
10 law to keep Plaintiff(s)'s and Class Members' Private Information confidential and to protect it
11 from unauthorized access and disclosure.

12 53. Convergent could have prevented this Data Breach by, among other things,
13 properly encrypting or otherwise protecting their equipment and computer files containing PII.

14 ***Defendant Acquires, Collects, and Stores Plaintiff(s)'s and Class Members' PII.***

15 54. Convergent acquires, collects, and stores a massive amount of PII of consumers
16 for its business purposes as it provides debt collection services to third-party businesses (*i.e.*,
17 Convergent's customers). Upon information and belief, Convergent may not be properly deleting
18 or destroying the PII records of its former customers or for those consumers whose debts have
19 been fully satisfied.

20 55. By obtaining, collecting, and using Plaintiff(s)' and Class Members' PII for its
21 own financial gain and business purposes, Defendant assumed legal and equitable duties and
22 knew that it was responsible for protecting Plaintiff(s)' and Class Members' PII from disclosure.

23 56. Plaintiff(s) and the Class Members have taken reasonable steps to maintain the
24 confidentiality of their PII.

57. Plaintiff(s) and the Class Members relied on Defendant to keep their PII

²¹ Notice Letter, Exhibit A.

1 confidential and securely maintained, to use this information for business purposes only, and to
2 make only authorized disclosures of this information.

3 ***The Data Breach was a***
4 ***Foreseeable Risk of which Defendant was on Notice***

5 58. It is well known that PII, including Social Security numbers in particular, is a
6 valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect
7 such information, including Convergent, are well-aware of the risk of being targeted by
8 cybercriminals.

9 59. Individuals place a high value not only on their PII, but also on the privacy of that
10 data. Identity theft causes severe negative consequences to its victims, as well as severe distress
11 and hours of lost time trying to fight against the impact of identity theft.

12 60. A data breach increases the risk of becoming a victim of identity theft. Victims of
13 identity theft can suffer from both direct and indirect financial losses. According to a research
14 study published by the Department of Justice, “[a] direct financial loss is the monetary amount
15 the offender obtained from misusing the victim’s account or personal information, including the
16 estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any
17 losses that were reimbursed to the victim. An indirect loss includes any other monetary cost
18 caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses
19 that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included
20 in the calculation of out-of-pocket loss.”²²

21 61. Individuals, like Plaintiff(s) and Class members, are particularly concerned with
22 protecting the privacy of their Social Security numbers, which are the key to stealing any person’s
23 identity and is likened to accessing your DNA for hacker’s purposes.

24 62. Data Breach victims suffer long-term consequences when their social security

²² “Victims of Identity Theft, 2018,” U.S. Department of Justice (April 2021, NCJ 256085) available at:
<https://bjs.ojp.gov/content/pub/pdf/vit18.pdf> (last accessed November 1, 2022).

1 numbers are taken and used by hackers. Even if they know their social security numbers are being
 2 misused, Plaintiff(s) and Class Members cannot obtain new numbers unless they become a victim
 3 of social security number misuse.

4 63. The Social Security Administration has warned that “a new number probably
 5 won’t solve all your problems. This is because other governmental agencies (such as the IRS and
 6 state motor vehicle agencies) and private businesses (such as banks and credit reporting
 7 companies) will have records under your old number. Along with other personal information,
 8 credit reporting companies use the number to identify your credit record. So using a new number
 9 won’t guarantee you a fresh start. This is especially true if your other personal information, such
 as your name and address, remains the same.”²³

10 64. In 2021, there were a record 1,862 data breaches last year, surpassing both 2020's
 11 total of 1,108 and the previous record of 1,506 set in 2017.²⁴

12 65. Additionally in 2021, there was a 15.1% increase in cyberattacks and data
 13 breaches since 2020. Over the next two years, in a poll done on security executives, they have
 14 predicted an increase in attacks from “social engineering and ransomware” as nation-states and
 15 cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely
 come from “misconfigurations, human error, poor maintenance, and unknown assets.”²⁵

16 66. In light of high-profile data breaches at other industry leading companies,
 17 including Microsoft (250 million records, December 2019), Wattpad (268 million records, June
 18 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January
 19 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion
 20 records, May 2020), Convergent knew or should have known that its computer network would
 be targeted by cybercriminals.

21
 22 ²³ <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed November 1, 2022).

23 ²⁴ <https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/> (last accessed November 1, 2022).

24 ²⁵ <https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864> (last accessed November 1, 2022).

67. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, and hopefully can ward off a cyberattack.

68. According to an FBI publication, “[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.”²⁶ This publication also explains that “[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn’t guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity.”²⁷

69. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep PII private and secure, Convergent failed to take appropriate steps to protect the PII of Plaintiff(s) and the proposed Class from being compromised.

70. Convergent failed to abide by its own Privacy Policy.²⁸

At All Relevant Times Convergent Had a Duty to Plaintiff(s) and Class Members to Properly Secure their Private Information

71. At all relevant times, Convergent had a duty to Plaintiff(s) and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff(s) and Class Members, and to promptly

²⁶ <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware> (last accessed November 1, 2022).

²⁷ *Id.*

²⁸ <https://www.convergentusa.com/outsourcing/page/privacy-policy#q2> (last accessed on November 1, 2022).

1 notify Plaintiff(s) and Class Members when Convergent became aware that their PII was
2 compromised.

3 72. Convergent had the resources necessary to prevent the Data Breach but neglected
4 to adequately invest in security measures, despite its obligation to protect such information.
5 Accordingly, Convergent breached its common law, statutory, and other duties owed to
6 Plaintiff(s) and Class Members.

7 73. Security standards commonly accepted among businesses that store PII using the
8 internet include, without limitation:

- 9 a. Maintaining a secure firewall configuration;
- 10 b. Maintaining appropriate design, systems, and controls to limit user access to
11 certain information as necessary;
- 12 c. Monitoring for suspicious or irregular traffic to servers;
- 13 d. Monitoring for suspicious credentials used to access servers;
- 14 e. Monitoring for suspicious or irregular activity by known users;
- 15 f. Monitoring for suspicious or unknown users;
- 16 g. Monitoring for suspicious or irregular server requests;
- 17 h. Monitoring for server requests for PII;
- 18 i. Monitoring for server requests from VPNs; and
- 19 j. Monitoring for server requests from Tor exit nodes.

20 74. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud
21 committed or attempted using the identifying information of another person without authority.”²⁹
22 The FTC describes “identifying information” as “any name or number that may be used, alone
23 or in conjunction with any other information, to identify a specific person,” including, among
24 other things, “[n]ame, Social Security number, date of birth, official State or government issued
driver’s license or identification number, alien registration number, government passport

²⁹ 17 C.F.R. § 248.201 (2013).

number, employer or taxpayer identification number.”³⁰

75. The ramifications of Convergent’s failure to keep consumers’ PII secure are long lasting and severe. Once PII is stolen, particularly Social Security and driver’s license numbers, fraudulent use of that information and damage to victims including Plaintiff(s) and the Class may continue for years.

The Value of Personal Identifiable Information

76. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200.³¹

77. Criminals can also purchase access to entire company’s data breaches from \$900 to \$4,500.³²

78. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual’s Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don’t pay the bills, it damages your credit. You may not find out that someone is using your number until you’re turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.³³

³⁰ *Id.*

³¹ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed November 1, 2022).

³² *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed November 1, 2022).

³³ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed November 1, 2022).

79. Attempting to change or cancel a stolen Social Security number is difficult if not nearly impossible. An individual cannot obtain a new Social Security number without evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

80. Even a new Social Security number may not be effective, as “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”³⁴

81. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market.”³⁵

82. PII can be used to distinguish, identify, or trace an individual’s identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother’s maiden name.³⁶

83. Given the nature of this Data Breach, it is foreseeable that the compromised PII can be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Class Members’ PII can easily obtain Class Members’ tax returns or open fraudulent credit card accounts in Class Members’ names.

84. The Private Information compromised in this Data Breach is static and difficult,

³⁴ Brian Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last accessed November 1, 2022).

³⁵ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed November 1, 2022).

³⁶ See OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1 (last accessed November 1, 2022).

1 if not impossible, to change (such as Social Security numbers).

2 85. Moreover, Convergent has offered only a limited subscription for identity theft
3 monitoring and identity theft protection through IDX. Its limitation is inadequate when IDX's
4 victims are likely to face many years of identity theft.

5 86. Furthermore, Defendant Convergent's credit monitoring offer and advice to
6 Plaintiff(s) and Class Members squarely places the burden on Plaintiff(s) and Class Members,
7 rather than on the Defendant, to monitor and report suspicious activities to law enforcement. In
8 other words, Convergent expects Plaintiff(s) and Class Members to protect themselves from its
9 tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff(s) and
10 Class Members in credit monitoring services upon discovery of the breach, Defendant merely
11 sent instructions to Plaintiff(s) and Class Members about actions they can affirmatively take to
12 protect themselves.

13 87. These services are wholly inadequate as they fail to provide for the fact that
14 victims of data breaches and other unauthorized disclosures commonly face multiple years of
15 ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for
16 the unauthorized release and disclosure of Plaintiff(s)' and Class Members' PII.

17 88. The injuries to Plaintiff(s) and Class Members were directly and proximately
18 caused by Convergent's failure to implement or maintain adequate data security measures for the
19 victims of its Data Breach.

20 ***Convergent Failed to Comply with FTC Guidelines***

21 89. Federal and State governments have established security standards and issued
22 recommendations to mitigate the risk of data breaches and the resulting harm to consumers and
23 financial institutions. The FTC has issued numerous guides for business highlighting the
24 importance of reasonable data security practices. According to the FTC, the need for data security

1 should be factored into all business decision-making.³⁷

2 90. In 2016, the FTC updated its publication, *Protecting Personal Information: A*
 3 *Guide for Business*, which established guidelines for fundamental data security principles and
 4 practices for business.³⁸ The guidelines note businesses should protect the personal consumer
 5 and consumer information that they keep, as well as properly dispose of personal information
 6 that is no longer needed; encrypt information stored on computer networks; understand their
 network's vulnerabilities; and implement policies to correct security problems.

7 91. The FTC emphasizes that early notification to data breach victims reduces
 8 injuries: "If you quickly notify people that their personal information has been compromised,
 9 they can take steps to reduce the chance that their information will be misused" and "thieves who
 10 have stolen names and Social Security numbers can use that information not only to sign up for
 11 new accounts in the victim's name, but also to commit tax identity theft. People who are notified
 early can take steps to limit the damage."³⁹

12 92. The FTC recommends that companies verify that third-party service providers
 13 have implemented reasonable security measures.⁴⁰

14 93. The FTC recommends that businesses:

- 15 a. Identify all connections to the computers where you store sensitive
- 16 information.
- 17 b. Assess the vulnerability of each connection to commonly known or
- 18 reasonably foreseeable attacks.
- 19 c. Do not store sensitive consumer data on any computer with an internet

20 ³⁷ Federal Trade Commission, *Start With Security*, available at:
 21 <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last accessed
 November 1, 2022).

22 ³⁸ Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at:
 23 <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>
 (last accessed November 1, 2022).

24 ³⁹ <https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business> (last accessed
 November 1, 2022).

⁴⁰ FTC, *Start With Security*, *supra* note 37.

1 connection unless it is essential for conducting their business.

- 2 d. Scan computers on their network to identify and profile the operating system
3 and open network services. If services are not needed, they should be disabled
4 to prevent hacks or other potential security problems. For example, if email
5 service or an internet connection is not necessary on a certain computer, a
6 business should consider closing the ports to those services on that computer
7 to prevent unauthorized access to that machine.
- 8 e. Pay particular attention to the security of their web applications—the software
9 used to give information to visitors to their websites and to retrieve
10 information from them. Web applications may be particularly vulnerable to a
11 variety of hack attacks
- 12 f. Use a firewall to protect their computers from hacker attacks while it is
13 connected to a network, especially the internet.
- 14 g. Determine whether a border firewall should be installed where the business's
15 network connects to the internet. A border firewall separates the network
16 from the internet and may prevent an attacker from gaining access to a
17 computer on the network where sensitive information is stored. Set access
18 controls—settings that determine which devices and traffic get through the
19 firewall—to allow only trusted devices with a legitimate business need to
20 access the network. Since the protection a firewall provides is only as
21 effective as its access controls, they should be reviewed periodically.
- 22 h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an
23 eye out for activity from new users, multiple log-in attempts from unknown
24 users or computers, and higher-than-average traffic at unusual times of the
day.
- i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly
large amounts of data being transmitted from their system to an unknown user.

1 If large amounts of information are being transmitted from a business'
2 network, the transmission should be investigated to make sure it is authorized.

3 94. The FTC has brought enforcement actions against businesses for failing to protect
4 consumer and consumer data adequately and reasonably, treating the failure to employ
5 reasonable and appropriate measures to protect against unauthorized access to confidential
6 consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade
7 Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify
8 the measures businesses must take to meet their data security obligations.

9 95. Because Class Members entrusted Convergent with their PII, Convergent had, and
10 has, a duty to the Plaintiff(s) and Class Members to keep their PII secure.

11 96. Plaintiff(s) and the other Class Members reasonably expected that when they
12 provide PII to Convergent (or to Convergent's customers), Convergent would safeguard their
13 PII.

14 97. Convergent was at all times fully aware of its obligation to protect the personal
15 and financial data of consumers, including Plaintiff(s) and members of the Class. Convergent
16 was also aware of the significant repercussions if it failed to do so. Its own Privacy Policies,
17 quoted above, acknowledges this awareness.

18 98. Convergent's failure to employ reasonable and appropriate measures to protect
19 against unauthorized access to confidential consumer data—including Plaintiff(s)' and Class
20 Members' first names, last names, addresses, and Social Security numbers, and other highly
21 sensitive and confidential information—constitutes an unfair act or practice prohibited by Section
22 5 of the FTCA, 15 U.S.C. § 45.

23 ***Plaintiff(s) and Class Members Have Suffered Concrete Injury as a Result of Defendant's***
24 ***Inadequate Security and the Data Breach it Allowed.***

99. Plaintiff(s) and Class Members reasonably expected that Defendant would
provide adequate security protections for their PII, and Class Members provided Defendant with
sensitive personal information, including their names, addresses, and Social Security numbers.

100. Defendant's poor data security deprived Plaintiff(s) and Class Members of the benefit of their bargain. Plaintiff(s) and other individuals whose PII was entrusted with Convergent understood and expected that, as part of that business relationship, they would receive data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff(s) and Class Members received data security that was of a lesser value than what they reasonably expected. As such, Plaintiff(s) and the Class Members suffered pecuniary injury.

101. Cybercriminals intentionally attack and exfiltrate PII to exploit it. Thus, Class Members are now, and for the rest of their lives will be, at a heightened and substantial risk of identity theft. Plaintiff(s) have also incurred (and will continue to incur) damages in the form of, inter alia, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

102. The cybercriminals who obtained the Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets" or on the "dark web." Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

103. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

104. As a direct and/or proximate result of Defendant's wrongful actions and/or

1 inaction and the resulting Data Breach, Plaintiff(s) and the other Class Members have been
 2 deprived of the value of their PII, for which there is a well-established national and international
 3 market.

4 105. Furthermore, PII has a long shelf-life because it contains different forms of
 5 personal information, it can be used in more ways than one, and it typically takes time for an
 6 information breach to be detected.

7 106. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data
 8 Breach have also placed Plaintiff(s) and the other Class Members at an imminent, immediate,
 9 and continuing increased risk of identity theft and identity fraud. Indeed, "[t]he level of risk is
 10 growing for anyone whose information is stolen in a data breach." Javelin Strategy & Research,
 11 a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places
 12 consumers at a substantial risk of fraud."⁴¹ Moreover, there is a high likelihood that significant
 13 identity fraud and/or identity theft has not yet been discovered or reported. Even data that have
 14 not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now
 15 possess Class Members' PII will do so at a later date or re-sell it.

16 107. As a result of the Data Breach, Plaintiff(s) and Class Members have already
 17 suffered injuries, and each are at risk of a substantial and imminent risk of future identity theft.

18 108. Although Convergent admits that the "the unauthorized actor deployed certain
 19 data extraction tools" on its computer systems. Cybercriminals actually exfiltrated the PII that
 20 was accessed.⁴²

21 *Plaintiff Guy's Experience*

22 109. Plaintiff Leo Guy is, and at all times relevant to this Complaint was, a resident
 23 and citizen of the State of New Hampshire.

24 ⁴¹ The Consumer Data Insecurity Report: Examining The Data Breach- Identity Fraud Paradigm In
 Four Major Metropolitan Areas, (available at
https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last
 accessed November 1, 2022).

⁴² See Notice Letter, Ex. A.

1 110. Plaintiff Guy is a consumer who is apparently affiliated with a debt collection
2 customer of Convergent. Convergent required that either its customer or Plaintiff Guy to provide
3 it with his PII. Convergent was provided with his personal information, including but not limited
4 to his Social Security number.

5 111. On or about October 31, 2022, Plaintiff Guy received the Notice of Data Breach
6 letter, which indicated that Convergent had known about the Data Breach for over 4 months. The
7 letter informed him that his critical PII was accessed by an “unauthorized actor.” The letter stated
8 that the extracted information included his “name, contact information, financial account
9 number, and Social Security number” but did not expand on whether additional information was
10 stolen as well. See Guy Notice of Data Breach Letter, attached as Exhibit A.

11 112. Plaintiff Guy is alarmed by the amount of his Personal Information that was stolen
12 or accessed, and even more by the fact that his Social Security number was identified as among
13 the breach data on Convergent’s computer system.

14 113. For a couple of months now, Plaintiff Guy has been receiving a combination of
15 around 20 spam calls and many spam emails per day. Many of the spam emails include adult
16 related material or CBD products. His email spam has increased at least ten times since August
17 2022, to the point that he now receives up to fifty or so a day. Prior to this time, he was not
18 receiving the troublesome calls and emails.

19 114. Plaintiff Guy is concerned that the spam calls and texts are being placed with the
20 intent of obtaining more personal information from him and committing identity theft by way of
21 a social engineering attack.

22 115. In response to Convergent’s Notice of Data Breach, Plaintiff will be required to
23 spend time dealing with the consequences of the Data Breach, which will continue to include
24 time spent verifying the legitimacy of the Notice of Data Breach, exploring credit monitoring
and identity theft insurance options, and self-monitoring his accounts. They realize they will
likely have to spend about an hour a week verifying financial accounts to check for fraudulent
activities. The time they are forced to spend monitoring and securing their accounts has been lost

1 forever and cannot be recaptured.

2 116. Immediately after receiving the Notice Letter, Plaintiff spent time discussing his
3 options with a law firm and has started to check his financial accounts in an effort to mitigate the
4 damage that has been caused by Convergent.

5 117. Plaintiff is very careful about sharing PII and has never knowingly transmitted
6 unencrypted PII over the internet or any other unsecured source.

7 118. Plaintiff suffered actual injury and damages as a result of the Data Breach.
8 Plaintiff would not have provided Convergent with their PII had Convergent disclosed that it
9 lacked data security practices adequate to safeguard PII.

10 119. Plaintiff suffered actual injury in the form of damages and diminution in the value
11 of his PII—a form of intangible property that they entrusted to Convergent (or its customer).

12 120. Plaintiff has suffered lost time, annoyance, interference, and inconvenience as a
13 result of the Data Breach and has anxiety and increased concerns for the loss of his privacy,
14 especially his Social Security number.

15 121. Plaintiff Guy reasonably believes that his Private Information may have already
16 been sold by the cybercriminals. Had he been notified of Convergent's breach in a timelier
17 manner, he could have attempted to mitigate his injuries.

18 122. Plaintiff Guy has suffered imminent and impending injury arising from the
19 substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII,
20 especially his Social Security number, being placed in the hands of unauthorized third-parties
21 and possibly criminals.

22 123. Plaintiff has a continuing interest in ensuring that his PII, which upon information
23 and belief remains backed up and in Convergent's possession, is protected and safeguarded from
24 future breaches.

CLASS ACTION ALLEGATIONS

124. Plaintiff(s) bring this action on behalf of themselves and on behalf of all other
persons similarly situated ("the Class").

1 125. Plaintiff(s) propose the following Class definition, subject to amendment as
2 appropriate:

3 All persons whose Private Information was maintained on Defendant Convergent
4 Outsourcing, Inc.'s computer systems and compromised in Convergent's June 2022
Data Breach.

5 126. Excluded from the Class are Defendant's officers and directors, and any entity in
6 which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys,
7 successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the
judiciary to whom this case is assigned, their families and Members of their staff.

8 127. Plaintiff(s) hereby reserves the right to amend or modify the class definitions with
9 greater specificity or division after having had an opportunity to conduct discovery.

10 128. Numerosity. The Members of the Class are so numerous that joinder of all of them
11 is impracticable. While the exact number of Class Members is unknown to Plaintiff(s) at this
12 time, based on information and belief, the Class consists of thousands of persons whose data was
compromised in Data Breach.

13 129. Commonality. There are questions of law and fact common to the Class, which
14 predominate over any questions affecting only individual Class Members. These common
15 questions of law and fact include, without limitation:

16 A. Whether Defendant unlawfully used, maintained, lost, or disclosed
17 Plaintiff(s)' and Class Members' Private Information;

18 B. Whether Defendant failed to implement and maintain reasonable security
19 procedures and practices appropriate to the nature and scope of the
20 information compromised in the Data Breach;

21 C. Whether Defendant's data security systems prior to and during the Data
Breach complied with applicable data security laws and regulations;

22 D. Whether Defendant's data security systems prior to and during the Data
23 Breach were consistent with industry standards;

24 E. Whether Defendant owed a duty to Class Members to safeguard their Private

Information;

F. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

G. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

H. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

I. Whether Plaintiff(s) and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

J. Whether Defendant's conduct was negligent;

K. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

L. Whether Defendant's acts, inactions, and practices complained of herein violated the Colorado data protection laws invoked below;

M. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

N. Whether Plaintiff(s) and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

130. Typicality. Plaintiff(s)' claims are typical of those of other Class Members because Plaintiff(s)'s Private Information, like that of every other Class member, was compromised in the Data Breach.

131. Adequacy of Representation. Plaintiff(s) will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff(s)' Counsel are competent and experienced in litigating Class actions.

132. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff(s) and Class Members, in that all the Plaintiff(s)' and Class Members' Private Information was stored on the same computer systems and unlawfully accessed in the same way.

1 The common issues arising from Defendant's conduct affecting Class Members set out above
 2 predominate over any individualized issues. Adjudication of these common issues in a single
 3 action has important and desirable advantages of judicial economy.

4 133. Superiority. A Class action is superior to other available methods for the fair and
 5 efficient adjudication of the controversy. Class treatment of common questions of law and fact
 6 is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most
 7 Class Members would likely find that the cost of litigating their individual claims is prohibitively
 8 high and would therefore have no effective remedy. The prosecution of separate actions by
 9 individual Class Members would create a risk of inconsistent or varying adjudications with
 10 respect to individual Class Members, which would establish incompatible standards of conduct
 11 for Defendant. In contrast, the conduct of this action as a Class action presents far fewer
 12 management difficulties, conserves judicial resources and the parties' resources, and protects the
 13 rights of each Class member.

14 134. Defendant has acted on grounds that apply generally to the Class as a whole, so
 15 that class certification, injunctive relief, and corresponding declaratory relief are appropriate on
 16 a Class-wide basis.

17 135. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for
 18 certification because such claims present only particular, common issues, the resolution of which
 19 would advance the disposition of this matter and the parties' interests therein. Such particular
 20 issues include, but are not limited to:

- 21 • Whether Defendant owed a legal duty to Plaintiff(s) and the Class to exercise due care in
 22 collecting, storing, and safeguarding their Private Information;
- 23 • Whether Defendant's security measures to protect its data systems were reasonable in
 24 light of best practices recommended by data security experts;
- Whether Defendant's failure to institute adequate protective security measures amounted
 to negligence;
- Whether Defendant failed to take commercially reasonable steps to safeguard consumer

1 Private Information; and

2 • Whether adherence to FTC data security recommendations, and measures recommended
3 by data security experts would have reasonably prevented the Data Breach.

4 136. Finally, all members of the proposed Class are readily ascertainable. Defendant
5 has access to Class Members' names and addresses affected by the Data Breach. Class Members
6 have already been preliminarily identified and sent notice of the Data Breach by Convergent.

7 **CAUSES OF ACTION**

8 **FIRST COUNT**

9 **Negligence**

10 **(On behalf of Plaintiff(s) and All Class Members)**

11 137. Plaintiff(s) re-allege and incorporate by reference the paragraphs above as if fully
12 set forth herein.

13 138. Convergent owed a duty to Plaintiff(s) and Class members to exercise reasonable
14 care in safeguarding and protecting their PII in its possession, custody, or control.

15 139. Plaintiff(s) and the Class Members entrusted their PII to Defendant with the
16 understanding that Defendant would safeguard their information.

17 140. Convergent had full knowledge of the sensitivity of the PII and the types of harm
18 that Plaintiff(s) and Class Members could and would suffer if the PII were wrongfully disclosed.

19 141. By assuming the responsibility to collect and store this data, and in fact doing so,
20 and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable
21 means to secure and safeguard its computer network—and Class Members' PII held within it—
22 to prevent disclosure of the information, and to safeguard the information from theft.
23 Defendant's duty included a responsibility to implement processes by which it could detect a
24 breach of its security systems in a reasonably expeditious period of time and to give prompt
notice to those affected in the case of a data breach.

142. Defendant had a duty to employ reasonable security measures under Section 5 of
the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or
affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of

1 failing to use reasonable measures to protect confidential data.

2 143. Defendant's duty to use reasonable care in protecting confidential data arose not
3 only as a result of the statutes and regulations described above, but also because Defendant is
4 bound by industry standards to protect confidential PII.

5 144. Defendant breached its duties, and thus was negligent, by failing to use reasonable
6 measures to protect Class Members' PII. The specific negligent acts and omissions committed
7 by Defendant include, but are not limited to, the following:

- 8 a. Failing to adopt, implement, and maintain adequate security measures to
9 safeguard Class Members' PII;
- 10 b. Failing to adequately monitor the security of its networks and systems;
- 11 c. Failing to periodically ensure that its email system had plans in place to
12 maintain reasonable data security safeguards;
- 13 d. Allowing unauthorized access to Class Members' PII; and
- 14 e. Failing to detect in a timely manner that Class Members' PII had been
15 compromised.

16 145. It was foreseeable that Defendant's failure to use reasonable measures to protect
17 Class Members' PII would result in injury to Class Members. Further, the breach of security was
18 reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the
19 industry.

20 146. It was therefore foreseeable that the failure to adequately safeguard Class
21 Members' PII would result in one or more types of injuries to Class Members.

22 147. There is a temporal and close causal connection between Defendant's failure to
23 implement security measures to protect the PII and the harm suffered, and an imminent and
24 substantial risk of harm that will be suffered by Plaintiff(s) and the Class.

148. As a result of Defendant's negligence, Plaintiff(s) and the Class Members have
suffered and will continue to suffer damages and injury including, but not limited to: out-of-
pocket expenses associated with procuring robust identity protection and restoration services;

1 increased risk of future identity theft and fraud, the costs associated therewith; time spent
 2 monitoring, addressing and correcting the current and future consequences of the Data Breach;
 3 and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

4 149. Plaintiff(s) and Class Members are entitled to compensatory and consequential
 5 damages suffered as a result of the Data Breach.

6 150. Plaintiff(s) and Class Members are also entitled to injunctive relief requiring
 7 Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit
 8 to future annual audits of those systems and monitoring procedures; and (iii) continue to provide
 9 adequate credit monitoring to all Class Members.

10 **SECOND COUNT**

11 ***Negligence Per Se***

12 **(On Behalf of Plaintiff(s) and All Class Members)**

13 151. Plaintiff(s) re-allege and incorporate by reference the paragraphs above as if fully
 14 set forth herein.

15 152. Section 5 of the FTCA prohibits "unfair . . . practices in or affecting commerce,"
 16 including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such
 17 as Defendant's, of failing to use reasonable measures to protect PII. The FTC publications and
 18 orders described above also form part of the basis of Defendants' duty in this regard.

19 153. Convergent violated Section 5 of the FTC Act by failing to use reasonable
 20 measures to protect PII and not complying with applicable industry standards. Defendants'
 21 conduct was particularly unreasonable given the nature and amount of PII it obtained and stored,
 22 and the foreseeable consequences of the Data Breach for companies of Defendants' magnitude,
 23 including, specifically, the immense damages that would result to Plaintiff(s) and Members of
 24 the Class due to the valuable nature of the PII at issue in this case—including Social Security
 numbers.

154. Defendants' violations of Section 5 of the FTCA constitute negligence per se.

155. Plaintiff(s) and members of the Class are within the class of persons that the FTCA

1 was intended to protect.

2 156. The harm that occurred as a result of the Data Breach is the type of harm the
3 FTCA was intended to guard against. The FTC has pursued enforcement actions against
4 businesses, which, as a result of their failure to employ reasonable data security measures and
5 avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff(s) and
6 members of the Class.

7 157. As a direct and proximate result of Defendant's negligence per se, Plaintiff(s) and
8 members of the Class have suffered and will suffer injury, including but not limited to: (i) actual
9 identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise,
10 publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention,
11 detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v)
12 lost opportunity costs associated with effort expended and the loss of productivity addressing and
13 attempting to mitigate the actual and future consequences of the Data Breach, including but not
14 limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud
15 and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued
16 risk to their PII, which remains in Defendants' possession and is subject to further unauthorized
17 disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect
18 the PII of customers in its continued possession; and (viii) future costs in terms of time, effort,
19 and money that will be expended to prevent, detect, contest, and repair the impact of the PII
20 compromised as a result of the Data Breach for the remainder of the lives of Plaintiff(s) and
21 members of the Class.

22 158. Additionally, as a direct and proximate result of Defendants' negligence per se,
23 Plaintiff(s) and members of the Class have suffered and will suffer the continued risks of
24 exposure of their PII, which remains in Defendants' possession and is subject to further
unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate
measures to protect the PII in their continued possession.

159. Plaintiff(s)' and Class Members' Personal Information constitutes personal

property that was stolen due to Convergent's negligence, resulting in harm, injury and damages to Plaintiff(s) and Class Members.

160. Convergent's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff(s)' and Class Members' unencrypted Personal Information.

161. Plaintiff(s) and Class Members have suffered and will continue to suffer damages as a result of Convergent's conduct. Plaintiff(s) and Class Members seek damages and other relief as a result of Convergent's negligence.

THIRD COUNT

Breach of Implied Contract

(On Behalf of Plaintiff(s) and All Class Members)

162. Plaintiff(s) re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

163. Plaintiff(s) and Class Members were required to provide their PII to Defendant as a condition of receiving other services provided by Defendant.

164. Plaintiff(s) and Class Members provided their PII to Defendant or its third-party agents in exchange for Convergent's services or employment. In exchange for the PII, Defendant promised to protect their PII from unauthorized disclosure.

165. At all relevant times Defendant promulgated, adopted, and implemented written a Privacy Policy whereby it expressly promised Plaintiff(s) and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

166. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff(s)' and Class Members' PII would remain protected.

167. Implicit in the agreement between Plaintiff(s) and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff(s) and Class Members with prompt and sufficient notice of any and all

1 unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of
2 Plaintiff(s) and Class Members from unauthorized disclosure or uses, (f) retain the PII only under
3 conditions that kept such information secure and confidential.

4 168. When Plaintiff(s) and Class Members provided their PII to Defendant as a
5 condition of relationship, they entered into implied contracts with Defendant pursuant to which
6 Defendant agreed to reasonably protect such information.

7 169. Defendant required Class Members to provide their PII as part of Defendant's
8 regular business practices.

9 170. In entering into such implied contracts, Plaintiff(s) and Class Members reasonably
10 believed and expected that Defendant's data security practices complied with relevant laws and
11 regulations and were consistent with industry standards.

12 171. Plaintiff(s) and Class Members would not have entrusted their PII to Defendant
13 in the absence of the implied contract between them and Defendant to keep their information
14 reasonably secure. Plaintiff(s) and Class Members would not have entrusted their PII to
15 Defendant in the absence of its implied promise to monitor its computer systems and networks
16 to ensure that it adopted reasonable data security measures.

17 172. Plaintiff(s) and Class Members fully and adequately performed their obligations
18 under the implied contracts with Defendant.

19 173. Defendant breached its implied contracts with Class Members by failing to
20 safeguard and protect their PII.

21 174. As a direct and proximate result of Defendant's breaches of the implied contracts,
22 Class Members sustained damages as alleged herein.

23 175. Plaintiff(s) and Class Members are entitled to compensatory and consequential
24 damages suffered as a result of the Data Breach.

176. Plaintiff(s) and Class Members are also entitled to nominal damages for the
breach of implied contract.

177. Plaintiff(s) and Class Members are also entitled to injunctive relief requiring

Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate long term credit monitoring to all Class Members for a period longer than the grossly inadequate one-year currently offered.

FOURTH COUNT

Unjust Enrichment

(On Behalf of Plaintiff(s) and All Class Members)

178. Plaintiff(s) re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

179. Plaintiff(s) and Class Members conferred a monetary benefit on Defendant in the form of the provision of their PII and Defendant would be unable to engage in its regular course of business without that PII.

180. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiff(s) and Class Members and accepted that monetary benefit.

181. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff(s)' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff(s) and Class Members by utilizing cheaper, ineffective security measures. Plaintiff(s) and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

182. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff(s) and Class Members, because Defendant failed to implement appropriate data management and security measures.

183. Defendant acquired the PII through inequitable means in that it failed to disclose

1 the inadequate security practices previously alleged.

2 184. If Plaintiff(s) and Class Members had known that Defendant had not secured their
3 PII, they would not have agreed to provide their PII to Defendant.

4 185. Plaintiff(s) and Class Members have no adequate remedy at law.

5 186. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class
6 Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft;
7 (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or
8 theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and
9 recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs
10 associated with effort expended and the loss of productivity addressing and attempting to mitigate
11 the actual and future consequences of the Data Breach, including but not limited to efforts spent
12 researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued
13 risk to their PII, which remain in Defendant's possession and is subject to further unauthorized
14 disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect
15 PII in their continued possession; and (vii) future costs in terms of time, effort, and money that
16 will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a
17 result of the Data Breach for the remainder of the lives of Plaintiff(s) and Class Members.

18 187. As a direct and proximate result of Defendant's conduct, Plaintiff(s) and Class
19 Members have suffered and will continue to suffer other forms of injury and/or harm.

20 188. Defendant should be compelled to disgorge into a common fund or constructive
21 trust, for the benefit of Plaintiff(s) and Class Members, proceeds that they unjustly received from
22 them.

23 **FIFTH COUNT**

24 **Declaratory Judgment**

(On Behalf of Plaintiff(s) and All Class Members)

189. Plaintiff(s) re-allege and incorporate by reference the paragraphs above as if fully
set forth herein.

1 190. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is
 2 authorized to enter a judgment declaring the rights and legal relations of the parties and grant
 3 further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here,
 4 that are tortious and violate the terms of the federal and state statutes described in this Complaint.

5 191. An actual controversy has arisen in the wake of the Convergent data breach
 6 regarding its present and prospective common law and other duties to reasonably safeguard its
 7 customers' Personal Information and whether Convergent is currently maintaining data security
 8 measures adequate to protect Plaintiff(s) and Class members from further data breaches that
 9 compromise their Private Information.

10 192. Plaintiff(s) allege that Convergent's data security measures remain inadequate.
 11 Plaintiff(s) will continue to suffer injury because of the compromise of their Private Information
 12 and remain at imminent risk that further compromises of their Private Information will occur in
 13 the future.

14 193. Pursuant to its authority under the Declaratory Judgment Act, this Court should
 15 enter a judgment declaring, among other things, the following:

- 16 a. Convergent continues to owe a legal duty to secure consumers' Private
 17 Information and to timely notify consumers of a data breach under the common
 18 law, Section 5 of the FTC Act, and various states' statutes;
- 19 b. Convergent continues to breach this legal duty by failing to employ reasonable
 20 measures to secure consumers' Private Information.

21 194. The Court also should issue corresponding prospective injunctive relief requiring
 22 Convergent to employ adequate security protocols consistent with law and industry standards to
 23 protect consumers' Private Information.

24 195. If an injunction is not issued, Plaintiff(s) and Class members will suffer
 irreparable injury, and lack an adequate legal remedy, in the event of another data breach at
 Convergent. The risk of another such breach is real, immediate, and substantial. If another breach
 at Convergent occurs, Plaintiff(s) and class members will not have an adequate remedy at law
 because many of the resulting injuries are not readily quantified and they will be forced to bring
 multiple lawsuits to rectify the same conduct.

1 196. The hardship to Plaintiff(s) and class members if an injunction does not issue
 2 exceeds the hardship to Convergent if an injunction is issued. Among other things, if another
 3 massive data breach occurs at Convergent, Plaintiff(s) and class members will likely be subjected
 4 to fraud, identify theft, and other harms described herein. On the other hand, the cost to
 5 Convergent of complying with an injunction by employing reasonable prospective data security
 6 measures is relatively minimal, and Convergent has a pre-existing legal obligation to employ
 such measures.

7 197. Issuance of the requested injunction will not do a disservice to the public interest.
 8 To the contrary, such an injunction would benefit the public by preventing another data breach
 9 at Convergent, thus eliminating the additional injuries that would result to Plaintiffs and the
 10 millions of consumers whose Private Information would be further compromised.

PRAYER FOR RELIEF

11 WHEREFORE, Plaintiff(s) pray for judgment as follows:

12 A. For an Order certifying this action as a class action and appointing Plaintiff(s) and
 13 their counsel to represent the Class;

14 B. For equitable relief enjoining Defendant from engaging in the wrongful conduct
 15 complained of herein pertaining to the misuse and/or disclosure of Plaintiff(s)' and Class
 16 Members' Private Information, and from refusing to issue prompt, complete and accurate
 17 disclosures of its Data Breach to Plaintiff(s) and Class Members;

18 C. For equitable relief compelling Defendant to utilize appropriate methods and
 19 policies with respect to consumer data collection, storage, and safety, and to disclose with
 specificity the type of Private Information compromised during the Data Breach;

20 D. For equitable relief requiring restitution and disgorgement of the revenues
 21 wrongfully retained as a result of Defendant's wrongful conduct;

22 E. For declaratory relief as requested;

23 F. Ordering Defendant to pay for lifetime credit monitoring services for Plaintiff(s)
 24 and the Class;

1 G. For an award of actual damages, compensatory damages, statutory damages, and
2 statutory penalties, in an amount to be determined, as allowable by law;

3 H. For an award of punitive damages, as allowable by law;

4 I. For an award of attorneys' fees and costs, and any other expense, including expert
5 witness fees;

6 J. Pre- and post-judgment interest on any amounts awarded; and

7 K. Such other and further relief as this Court may deem just and proper.

8 DATED this 2nd day of November 2022.

9 **FRANK FREED SUBIT & THOMAS LLP**

10 By: /s/ Michael C. Subit

11 Michael C. Subit, WSBA #29189

12 705 Second Avenue, Suite 1200

13 Seattle, WA 98104

14 Telephone: 206.624.6711

15 msubit@frankfreed.com

16 *Local Counsel for Plaintiff(s)*

17 **MASON LLP**

18 Gary E. Mason*

19 Danielle L. Perry*

20 Lisa A. White*

21 5101 Wisconsin Avenue, NW, Suite 305

22 Washington, DC 20016

23 Telephone: 202.429.2290

24 gmason@masonllp.com

dperry@masonllp.com

lwhite@masonllp.com

Attorneys for Plaintiff(s)

**pro hac vice applications for admission to be filed.*